RSAC 2025 Conference

Many Voices.
One Community.

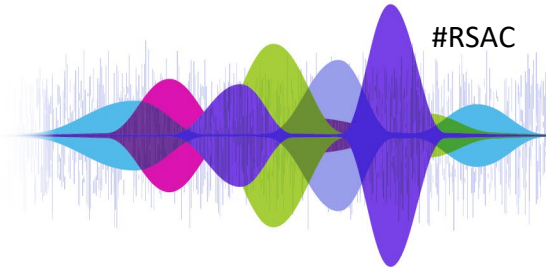
SESSION ID: PART1-T02

Redefining Universal ZTNA

Security and resilience for all users and things

April 29, 2025

Raj Chopra, SVP of Security Products, Cisco
Prabhu Barathi, Director, Global Security Technologist, Cisco



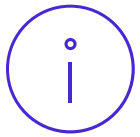
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Zero Trust must be defined holistically


Principles

Strategy

Architecture

Capabilities

Technologies

Features

Zero Trust principles

1. Never assume trust
2. Always verify
3. Enforce least privilege

Zero Trust success factors

1. Least privilege, not least convenient
2. Adapt policy to risk
3. Consistency across environments

Cisco Confidential

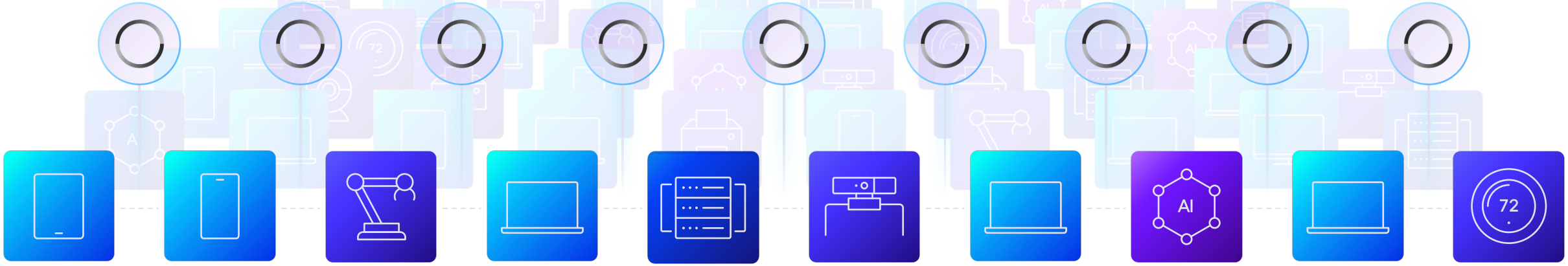
Cisco Confidential

AI
72
X

AI
72
AI
AI
72

Assess every
connection every time.
AI
AI
72

CONTINUOUS VALIDATION ACROSS ENTIRE CHAIN



Modern application access has transformed

GenAI apps

- AI Security and Security for AI
- Discover Shadow AI
- Enforce safety, security, privacy, and governance

Identity of users & things

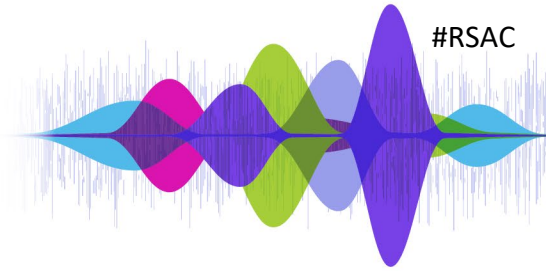
- Identity is foundation of zero trust
- Verify trust without friction
- Things are people too

Network & security convergence

- Security closer to the edge
- Modernize and unify with SASE
- Build operational resilience

In this brave new world, how do we verify and carry trust across every access scenario?

The ideal: Universal ZTNA



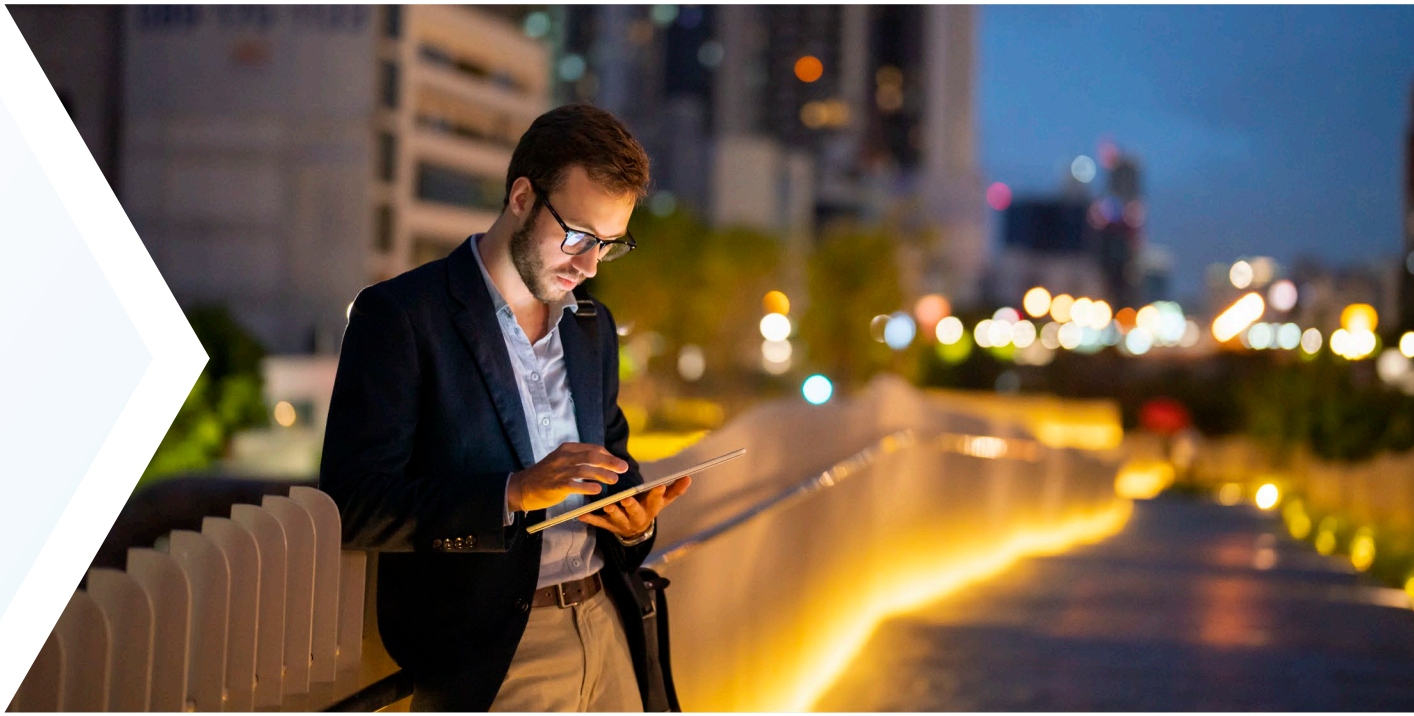
Seamless access to all apps

Identity Intelligence for users & things

Zero downtime zero trust

Flexible enforcement powered by AI for Security and Security for AI

Traditional ZTNA was designed for a different time and different needs



Universal ZTNA

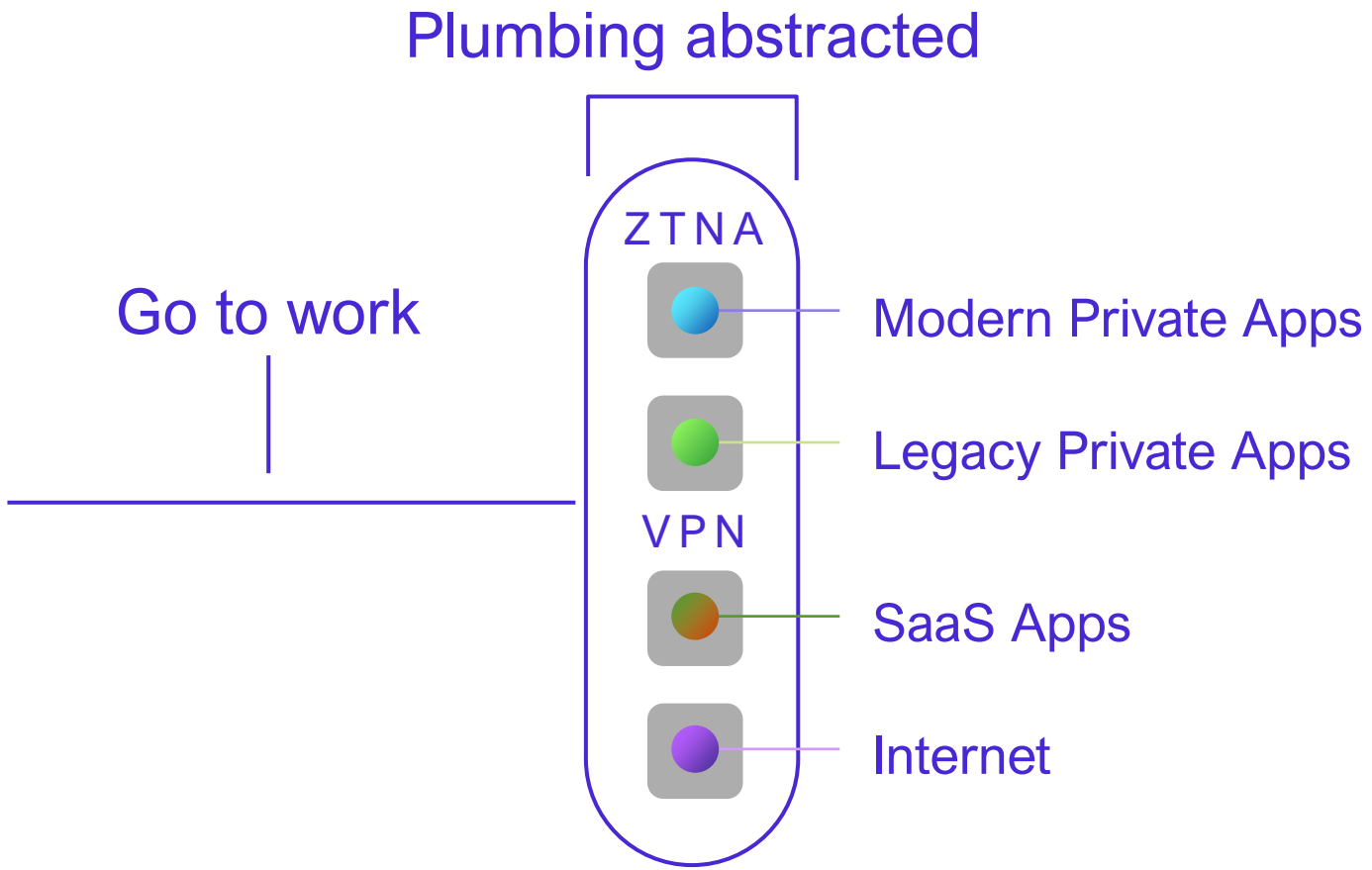
Answers: Can this user/thing be trusted? Are they who they say they are?

Ideal outcome: Seamless, secure access to all apps

Success criteria:

- Improve user experience – great performance in all locations
- Unify management and evolve to ZTNA at controlled pace
- Allow controlled, safe use of AI

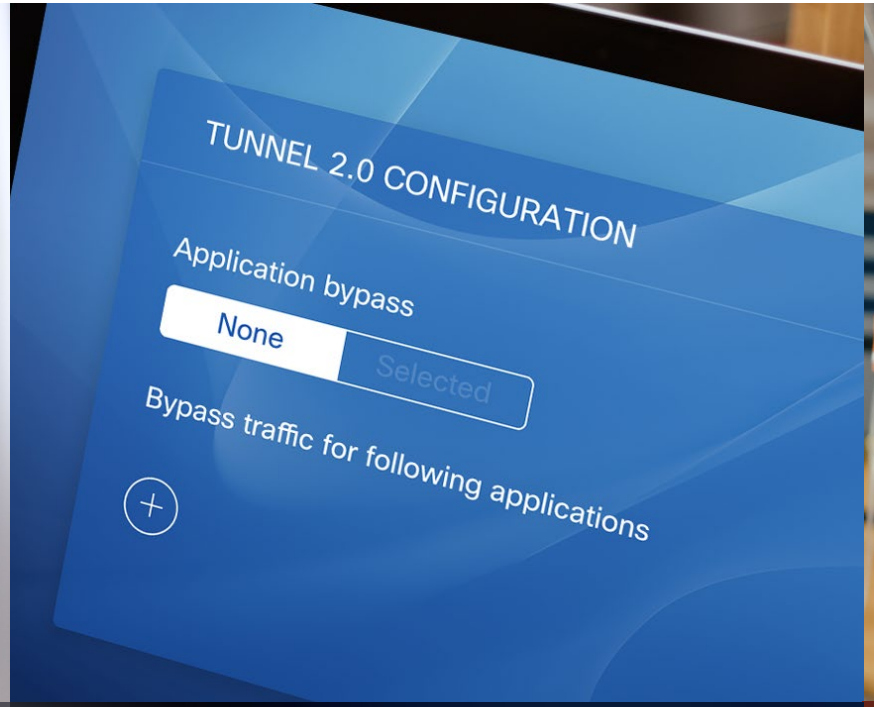
Seamless experience



The importance of performance… everywhere

MASQUE / QUIC / parallel processing / global peering

Faster than VPN on a plane



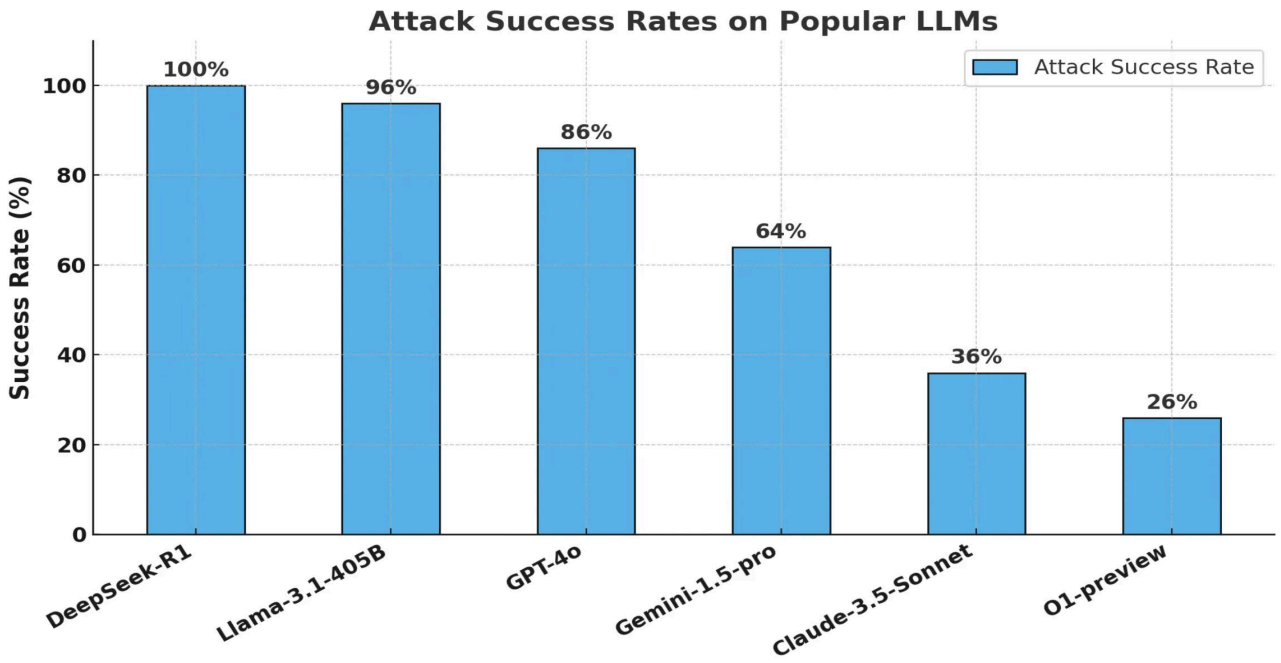
No application bypass needed

High performance for the field

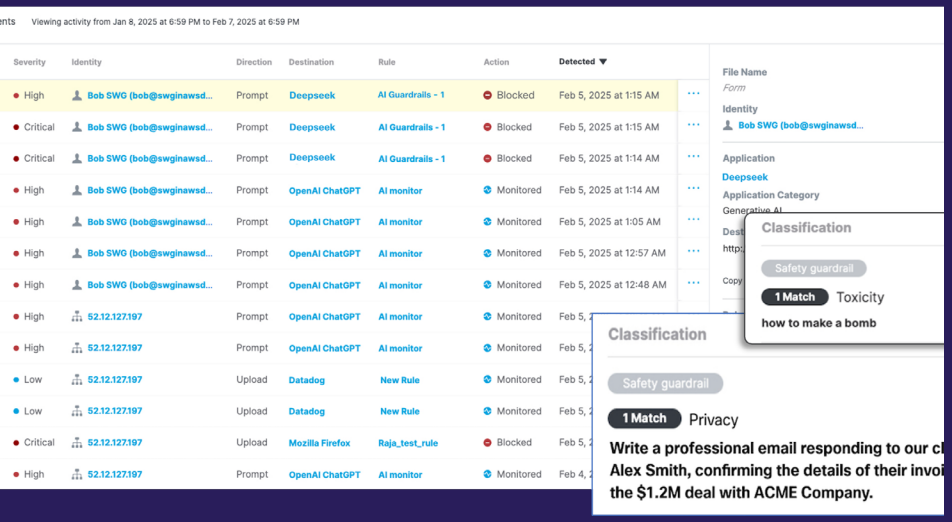
The importance of intent in AI safety and security

Advanced guardrails

- Mitigates prompt injections, toxic content
- Aligns with Mitre Atlas
- Compensating control for insecure LLMs



RSAC 2025 Conference


Viewing activity from Jan 8, 2025 at 6:59 PM to Feb 7, 2025 at 6:59 PM
Severity
Identity
Direction
Destination
Rule
Action
Detected
High Bob SWG (bob@swginawsd... Prompt Deepseek AI Guardrails - 1 Blocked Feb 5, 2025 at 1:15 AM
Critical Bob SWG (bob@swginawsd... Prompt Deepseek AI Guardrails - 1 Blocked Feb 5, 2025 at 1:15 AM
Critical Bob SWG (bob@swginawsd... Prompt Deepseek AI Guardrails - 1 Blocked Feb 5, 2025 at 1:14 AM
High Bob SWG (bob@swginawsd... Prompt OpenAI ChatGPT AI monitor Monitored Feb 5, 2025 at 1:14 AM
High Bob SWG (bob@swginawsd... Prompt OpenAI ChatGPT AI monitor Monitored Feb 5, 2025 at 1:05 AM
High Bob SWG (bob@swginawsd... Prompt OpenAI ChatGPT AI monitor Monitored Feb 5, 2025 at 12:57 AM
High Bob SWG (bob@swginawsd... Prompt OpenAI ChatGPT AI monitor Monitored Feb 5, 2025 at 12:48 AM
High 52.12.127.197 Prompt OpenAI ChatGPT AI monitor Monitored
High 52.12.127.197 Prompt OpenAI ChatGPT AI monitor Monitored
Low 52.12.127.197 Upload Datadog New Rule Monitored
Low 52.12.127.197 Upload Datadog New Rule Monitored
Critical 52.12.127.197 Upload Mozilla Firefox Raja_test_rule Blocked Feb 5,
High 52.12.127.197 Prompt OpenAI ChatGPT AI monitor Monitored Feb 4,
File Name
Form
Identity
Bob SWG (bob@swginawsd...
Application
Deepseek
Application Category
Classification
Safety guardrail
1 Match Toxicity
how to make a bomb
Classification
Safety guardrail
1 Match Privacy
Write a professional email responding to our cl
Alex Smith, confirming the details of their invoi
the $1.2M deal with ACME Company.

AI Access / Guardrails Demo

Many Voices.
One Community.

Ideal outcome: Improved identity protection

Success criteria:

- Increase identity security visibility and hygiene
- Leverage identity data to granularly secure users, devices, and IOT things
- Verify trust dynamically (e.g as users move) - with a good user experience

Identity and Context

Continuously assess you are who you say you are

BLIN RUST

User trust is dynamic

TRUSTED NEUTRAL UNTRUSTED

SAMANTHA JONES

Group: Staff

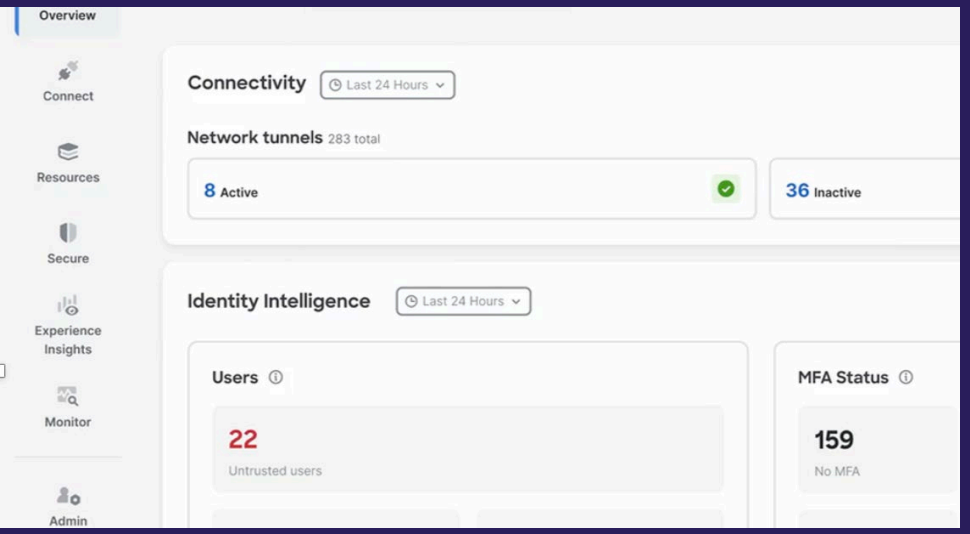
Logs in as Samantha_Jones

Accesses group_exec

Upgrades privileges to SuperAdmin

Attempts to access Billing_DB

RSAC 2025 Conference



Identity Intelligence Demo

Many Voices.
One Community.

Ideal outcome: Operational resilience, driving to zero downtime

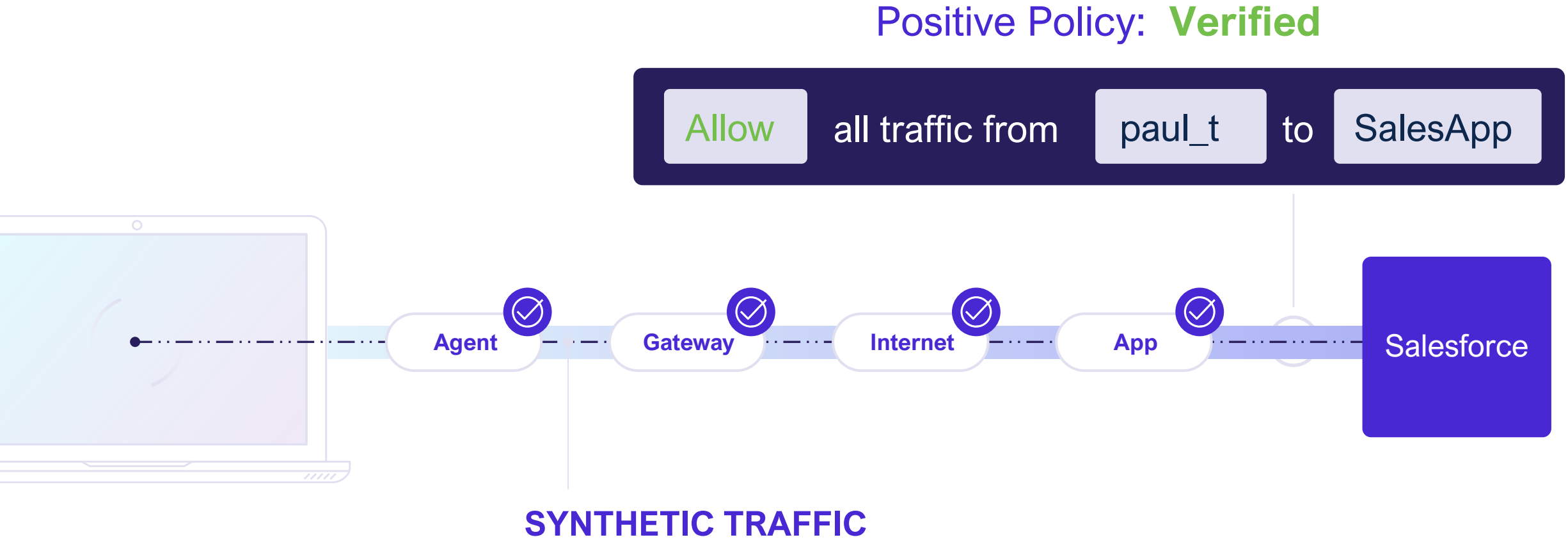
Success criteria:

- High performance and availability fuels high productivity
- End-to-end visibility for rapid detection/remediation
- Proactive policy testing to avoid conflicts

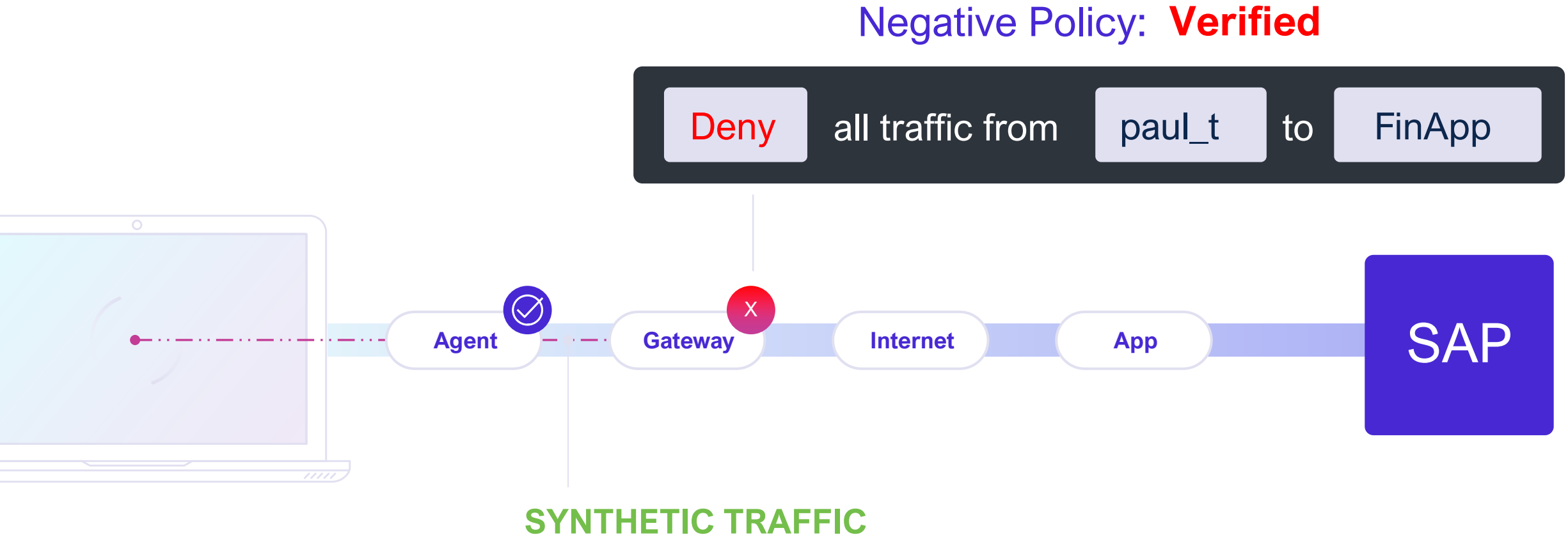
of outages are from misconfigurations

Cisco Confidential

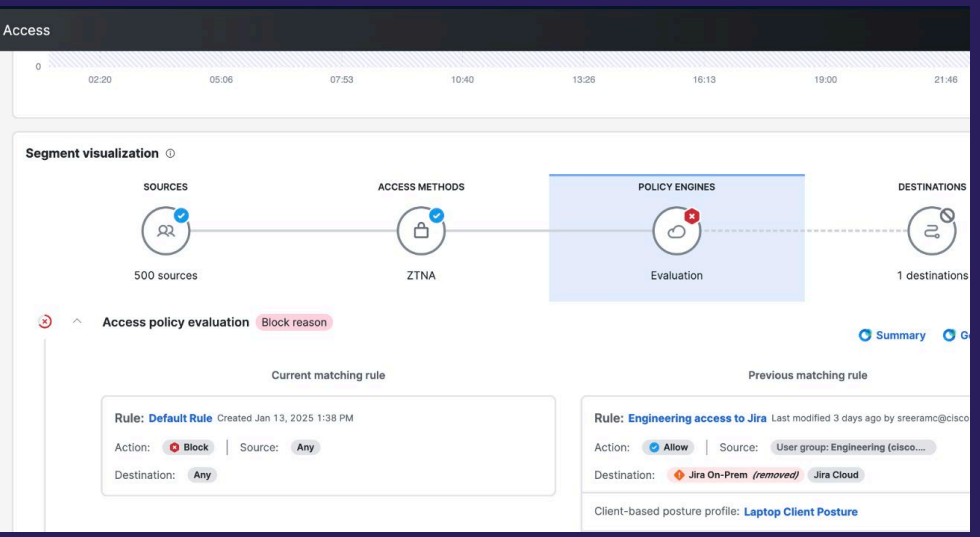
The importance of policy verification



The importance of policy verification



RSAC™ 2025 Conference

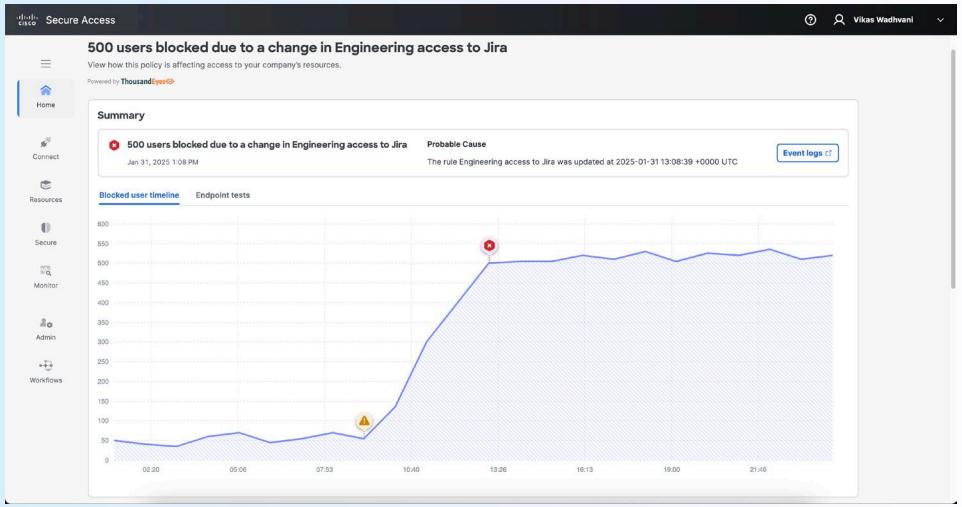


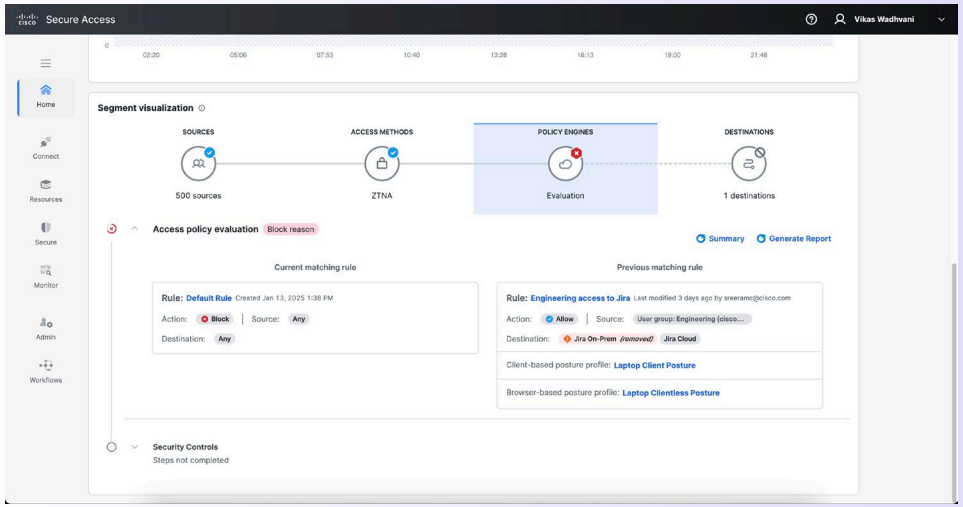
Policy Assurance “Preview” Demo

Many Voices.
One Community.

Policy Assurance*

FUTURE

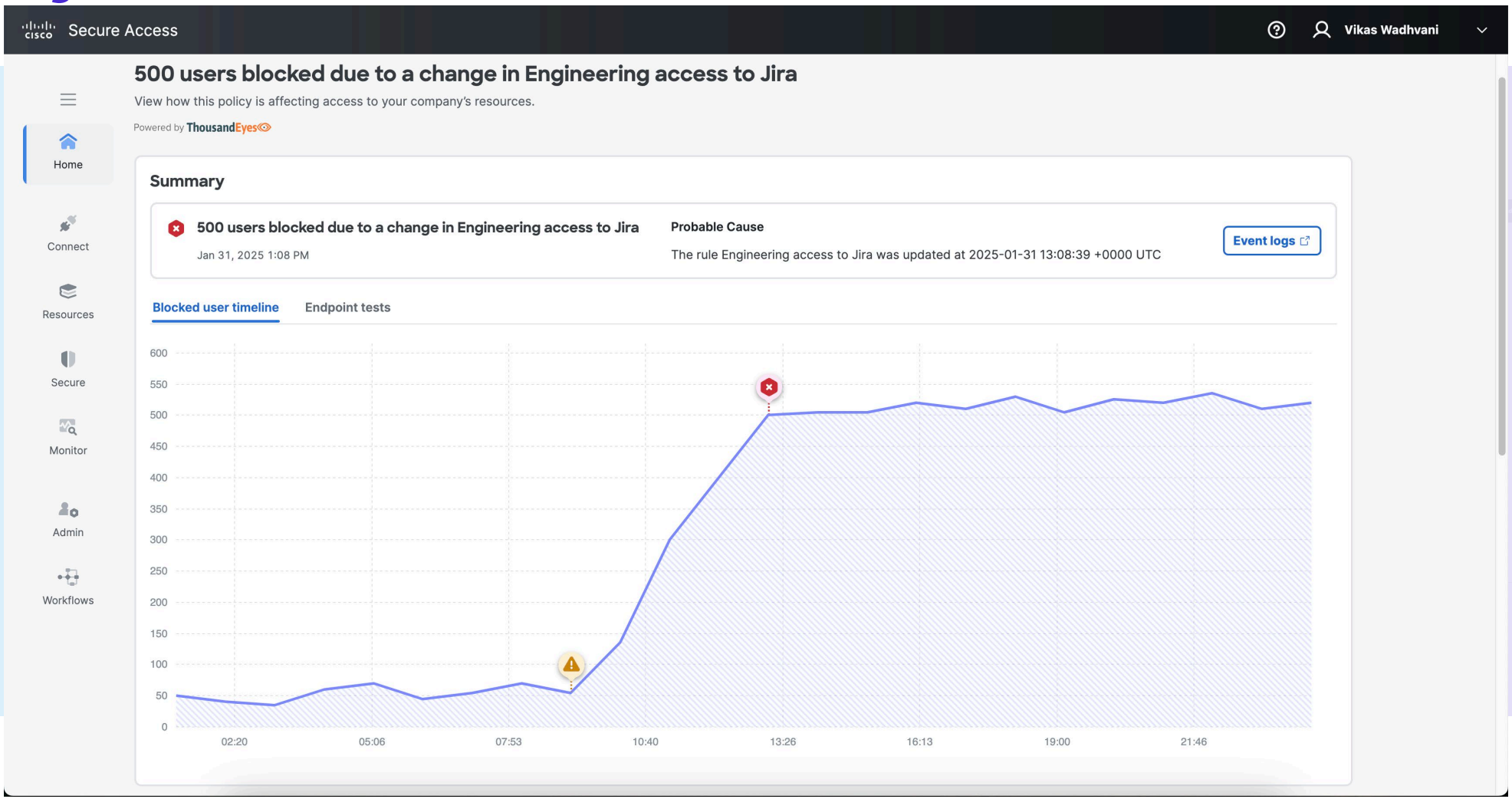

Secure Access
Vikas Wadhvani
500 users blocked due to a change in Engineering access to Jira
View how this policy is affecting access to your company's resources.
Summary
500 users blocked due to a change in Engineering access to Jira
Jan 31, 2025 1:08 PM
Probable Cause
The rule Engineering access to Jira was updated at 2025-01-31 13:08:39 +0000 UTC
Event logs
Blocked user timeline
Endpoint tests



* Capabilities are planned but not yet available or guaranteed.

FUTURE

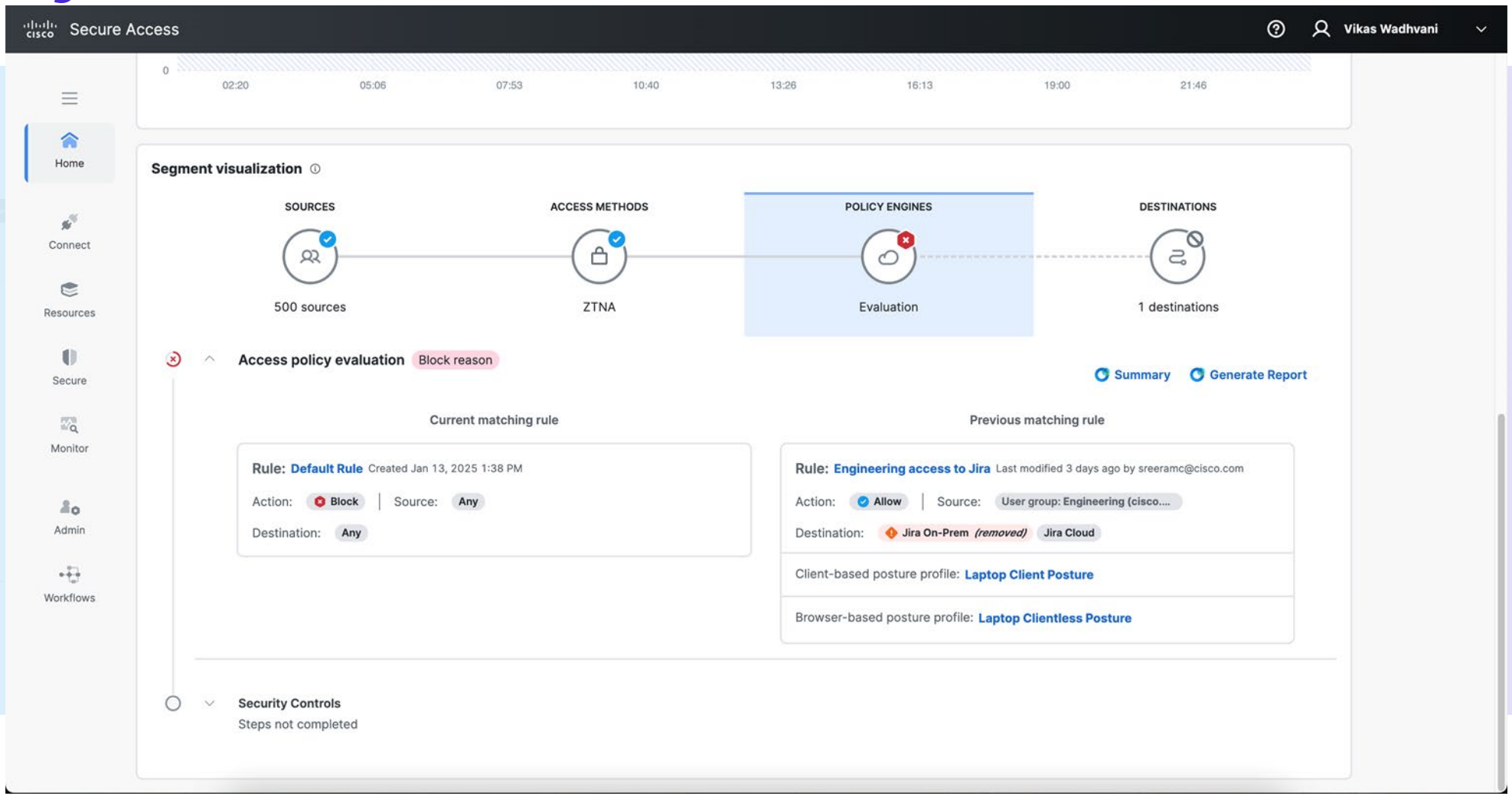
Policy Assurance*



* Capabilities are planned but not yet available or guaranteed.

FUTURE

Policy Assurance*



* Capabilities are planned but not yet available or guaranteed.

Cisco Confidential

RSAC 2025 Conference

Summary

Cisco IT’s zero trust journey

Compelling ROI with the zero-trust model

$3.4M

Annual savings in employee productivity[1]

$500K

Annual savings in IT helpdesk support costs[2]

86K

Potential compromises averted per month[3]

Source: Cisco IT based on the implementation of a zero-trust framework

1. As a result of 410,000 fewer VPN authentications per year
2. With <1% users contacting IT help desk vs 7% for typical security technology rollouts
3. 86,000 vulnerable devices self-remediated/month based on 5.76M device health checks/month

Apply What You Have Learned Today

Start with Discovery

Map key flows and components of Zero Trust Access environment

Next 3 Months: Assessment

Monitor cyber hygiene, determine which apps are ZTNA-ready vs VPN-as-a-service

Within 6 months: Enforce & Optimize

Enforce control on critical apps, measure progress, expand identity context from users to things.

cisco

RSAC 2025 Conference

Cisco Confidential

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You